Quantum logic gate constructions with one-bit "teleportation"

Xinlan Zhou[1,2*], Debbie W. Leung[3,2†], and Isaac L. Chuang[2‡]

[1] *Applied Physics Department*
Stanford, CA 94305-4090

[2] *IBM Almaden Research Center, 650 Harry Road*
San Jose, CA 95120

[3] *Quantum Entanglement Project, ICORP, JST*
Edward Ginzton Laboratory, Stanford University,
Stanford, CA 94305-4085

(February 22, 2000)

We present a general method to construct quantum logic gates using one-bit "teleportation" as a basic primitive, extending previous results based on traditional two-bit teleportation (D. Gottesman and I. L. Chuang, Nature **402**, 390, 1999). This allows the realization of a variety of useful quantum operations that cannot be directly performed due to some physical constraints. In particular, this technique leads to straightforward and systematic construction of many fault-tolerant encoded operations, including the $\pi/8$ and Toffoli gates, and remote quantum operations.

I. INTRODUCTION

Practical realization of quantum information processing requires specific types of quantum operations which may be difficult to construct, given available primitives. In particular, to robustly perform quantum computation in the presence of noise, one needs fault-tolerant implementations of quantum gates acting on states which are block–encoded using quantum error correcting codes. [1–4]. Fault-tolerant quantum gates must prevent propagation of single qubit errors to other qubits within the same block, so that small correctable errors will not grow to exceed the correction capability of the code. This requirement greatly restricts the types of unitary operations which can be performed on the encoded qubits. Certain fault-tolerant operations can be implemented easily by performing direct *transversal* operations on the encoded qubits, in which each qubit in a block interacts only with one corresponding qubit, either in another block or in a specialized ancilla. Unfortunately, for a given code, only a few useful operations can be accomplished transversally, and these are not universal, in that they cannot be composed to approximate an arbitrary quantum circuit. To obtain a universal set of gates, additional gates have to be constructed using ancilla states and measurements. This has been accomplished successfully [1,3,5,6]; unfortunately, however, these *ad-hoc* constructions are complicated and are not easily generalized.

Another application in which we are challenged to construct useful quantum operations from a limited set of primitives is in distributed quantum information processing. In this problem, certain kinds of communication between different parties are constrained or prohibited, but prior distribution of standard states may be allowed. For example, quantum teleportation [7] demonstrates how an unknown quantum state can be sent between two parties without sending any quantum information, using only classical communication and prior entanglement. Protocols for distributed state preparation and computation are also known [8], but again, they have largely been constructed by hand and offer neither an explanation of why a particular ancilla state is required, nor a systematic path for generalization.

A general framework for addressing such problems has been presented in [9]; it uses quantum teleportation as a basic primitive to enable construction of quantum operations which cannot be directly performed through unitary operations. This framework provides systematic and generalizable constructions for an infinite family of fault-tolerant gates, including the $\pi/8$ and Toffoli gates. However, it does not lead to circuits equivalent to (or as simple as) prior *ad-hoc* constructions for the same gates.

Here, we provide an extension to the teleportation method of gate construction, which utilizes a simpler primitive, which we call one-bit "teleportation." This method simplifies the constructions of [9], and furthermore provides strikingly unified constructions of the $\pi/8$, controlled-phase, and Toffoli gates. The circuit for the Toffoli gate is exactly the same as Shor's original construction [1]. We also find constructions for an infinite family of gates which are useful in the quantum factoring algorithm [11].

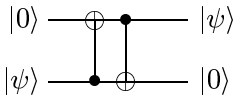
*Electronic address: xlz@snow.stanford.edu
†Electronic address: wcleung@leland.stanford.edu
‡Electronic address: ichuang@almaden.ibm.com

The structure of the paper is as follows. First, in Section II, we define one-bit teleportation, and describe its properties and various guises. Its application to fault-tolerant gate construction is presented in Section III, which is followed in Section IV with specific circuits for the $\pi/8$, controlled-phase, and Toffoli gates. In Section V, we use one-bit teleportation to derive the two-bit quantum teleportation protocol, and to construct a remote quantum gate. Finally, we summarize our results in Section VI.

II. ONE-BIT TELEPORTATION

Traditional quantum teleportation enables transmission of a qubit between a sender and a receiver without requiring a quantum operation to be performed jointly by the two parties. They need only begin with a certain entangled state, and communicate classical information. The same objective, communicating a qubit, can be accomplished in a simpler manner if the sender and receiver are allowed to perform a quantum gate (such as a controlled-NOT gate, a CNOT) between their respective qubits. We derive such one-bit "teleportation" circuits using the following facts:

- **Fact 1:** An unknown qubit state $|\psi\rangle$ can be swapped with the state $|0\rangle$ using only two CNOT gates, as shown in the following circuit



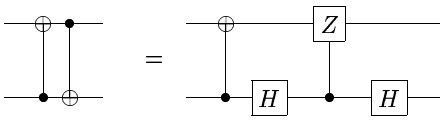
(1)

  Note that in all circuits we show, time proceeds from left to right as is usual, and conventions are as in [12]. Throughout this section, the first and second qubits refer to the registers with respective initial states $|0\rangle$ and $|\psi\rangle$.

- **Fact 2:** $X = HZH$, where X and Z are Pauli operators, and H is the Hadamard gate defined as

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{2}$$

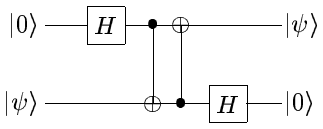
  Thus, the following two circuits are equivalent:



(3)

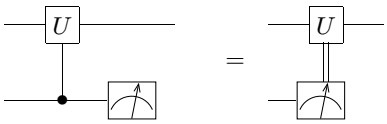
- **Fact 3:** Hadamard gates H acting on both qubits before and after a CNOT reverse its direction.

  Using fact 3 on both CNOTs in the circuit of Eq. (1) and relabelling $H|\psi\rangle$ as $|\psi\rangle$, one can obtain the following circuit:



(4)

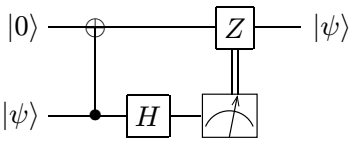
- **Fact 4:** Measurement commutes with a controlled-quantum gate when the control qubit is being measured:



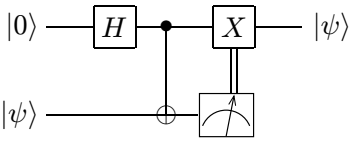
(5)

  The meter represents measurement of the Pauli operator Z, which projects the measured state onto $|0\rangle$ or $|1\rangle$. The double line coming out of the meter carries the one-bit classical measurement result, and U is performed if the measurement result is $|1\rangle$. Operations which are performed conditioned on classical measurement results are called classically-controlled operations in this paper.

In Eqs. (3) and (4), the two qubits are disentangled before the second Hadamard gate. Therefore, the second qubit can be measured without affecting the unknown state of the first qubit. Applying fact 4 to Eqs. (3) and (4) results in the one-bit teleportation circuits in Eqs. (6) and (7) respectively.

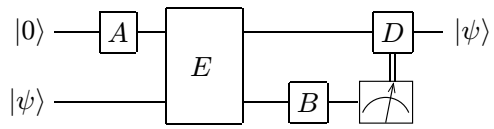


(6)



(7)

The circuit in Eq. (6) is referred to as "Z-teleportation," since a classically-controlled-Z is applied after measurement. Similarly, the circuit in Eq. (7) is referred to as "X-teleportation." X and Z-teleportation circuits can both be represented using the same general structure:



(8)

where for Z-teleportation, $A = I, B = H, D = Z$, and E is a single CNOT with the first qubit as its target (I is the 2×2 identity operator). For X-teleportation, $A = H, B = I, D = X$, and E is a single CNOT with the first qubit as its control.

The X and Z teleportation circuits are special cases of a more general circuit for teleportation discussed in Appendix A. We will mainly focus on the simpler circuits of X and Z teleportation which are sufficient for the constructions in this paper.

III. FAULT-TOLERANT GATE CONSTRUCTIONS USING ONE-BIT TELEPORTATION

In this section, we develop a general method for fault-tolerant gate construction using one-bit teleportation as a basic primitive. We will confine our attention to the CSS codes [13,14], although the results can be extended to any stabilizer codes [9].

A. Fault-tolerant gate hierarchy

We first summarize the fault-tolerant gate hierarchy introduced in [9]. Let C_1 represent the Pauli group; C_2, the Clifford group, is the set of gates which map Pauli operators into Pauli operators under conjugation. Elements in C_2 can be performed transversally on the states encoded in a CSS code [1,15,5]. Note that $C_1 \subset C_2$, and C_2 contains important gates which are not in C_1, such as the CNOT, the Hadamard gate H, and the phase gate S ($S|x\rangle = i^x|x\rangle$ for $x = \{0, 1\}$).

We can recursively define an infinite class of quantum gates as

$$C_k \equiv \{U | UC_1U^\dagger \subseteq C_{k-1}\}, \tag{9}$$

for $k \geq 2$. The $k = 2$ case reduces to the definition of the Clifford group. For every k, $C_k \supset C_{k-1}$, and $C_k - C_{k-1}$ is nonempty. In other words, the C_k is a strictly increasing family, and each C_k adds more interesting gates in the hierarchy. The C_3 gates which are not in C_2 are especially important, as Clifford group operations alone do not allow universal quantum computation, but adding a single gate in $C_3 - C_2$, such as the $\pi/8$ gate T, ($T|x\rangle = e^{i\pi x/4}|x\rangle$ for $x \in \{0, 1\}$), the controlled-phase gate $\Lambda_1(S)$ ($\Lambda_1(S)|xy\rangle = i^{x\cdot y}|xy\rangle$ for $x, y = \{0, 1\}$) or the Toffoli gate (controlled-controlled-NOT), to the Clifford group will give a universal set of unitary operations [1,16,6].

In contrast to the Clifford group operations, the elements in C_3 cannot be constructed using unitary transversal operations, and are more difficult to perform on an unknown encoded states. On the other hand, it is relatively easy to "perform" C_3 gates on known states having stabilizers in the Pauli group, by direct preparation of the (known) final states. A state with stabilizers $M_i \in C_1$ is transformed by $U \in C_3$ to the intended final state with stabilizers $UM_iU^\dagger$ which are in C_2 by definition [15]. These new stabilizers can be measured fault-tolerantly [1,17,5,9], allowing the final state to be created fault-tolerantly by measuring the stabilizers. This property will later be used in our fault-tolerant gate construction.

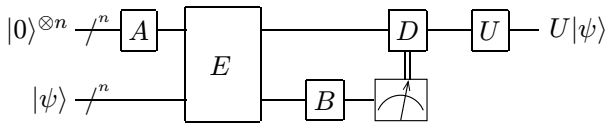
B. C_3 gate construction using one-bit teleportation

We now consider a general method to construct fault-tolerant gates in C_3 using the one-bit teleportation scheme as a primitive, which reduces the problem of applying C_3 gates to an arbitrary state to preparing a specific ancilla with stabilizers in C_2. Throughout the discussion, it is assumed that elements in C_2 can easily be performed and measured transversally.

The basic idea is the following. A trivial way to apply a quantum gate U to a state $|\psi\rangle$ is to first "teleport" $|\psi\rangle$ as in Sec. II and then apply U to the teleported $|\psi\rangle$. This extra teleportation step does not seem particularly useful, but it actually reduces the problem of fault-tolerant gate construction to fault-tolerant preparation of particular ancilla state. The main reason is that U is applied to the teleported state, which is originally the known ancilla state. If U can be commuted backwards without introducing more complicated gates, U is in effect applied to the known ancilla, which can be "performed" directly.

This idea has been used in [9], with two-bit teleportation as a primitive, to perform universal quantum computation. Both one-bit and two-bit teleportation reduce fault tolerant C_3 gate constructions to circuits composed of fault tolerant C_2 gates only. Two-bit teleportation, however, requires entangling measurements and some entangled initial ancilla states, which may complicate gate constructions. In contrast, one-bit teleportation only requires projective measurements of the Pauli operator Z on individual qubits and product initial ancilla states.

We now detail the formal construction. Let $U \in C_3$ be an n-qubit gate, to be applied to $|\psi\rangle$, an encoded quantum state with n *logical* qubits. We first teleport each logical qubit using either Z-teleportation or X-teleportation, in a bitwise manner. This swaps $|\psi\rangle$ with an ancilla prepared in the $|0\rangle^{\otimes n}$ state. We then apply U to the resulting teleported state to obtain $U|\psi\rangle$. This is described by the following quantum circuit:

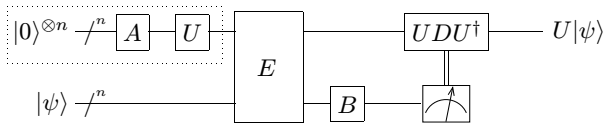


(10)

In Eq. (10), a register (wire) with the symbol "$/^n$" represents a bundle of n logical qubits. The measurement box measures Z bitwise and the double line represents

the n-bit classical outcome. The i^{th} classical bit controls whether an operator D_i is perform on the i^{th} logical state in the first register. This is represented by D for simplicity in Eq. (10). A is a bitwise operation, $A = A_1 \otimes \cdots \otimes A_n$, where A_i acts on the i^{th} logical qubit only. B is a bitwise operation similar to A. E is given by $E = E_i \otimes \cdots \otimes E_n$, where each E_i is a CNOT between the i^{th} logical qubits of $|\psi\rangle$ and the known ancilla. According to Sec. II, if Z-teleportation is applied to the i^{th} logical qubit, then, $A_i = I, B_i = H, D_i = Z$, and E_i is a CNOT with the first qubit as its target; if X-teleportation is applied instead, $A_i = H, B_i = I, D_i = X$, and E_i is a CNOT with the first qubit as its control.

We now commute U backwards in time. Commuting U with the classically-controlled operation D changes D to $UDU^\dagger$. Since $D \in C_1$ and $U \in C_3$, $UDU^\dagger \in C_2$ can still be performed transversally. Likewise, commuting U with E changes E to $UEU^\dagger$ [10]. However, as CNOT $\notin C_1$, the resulting operation $UEU^\dagger$ may not be in C_2 for an arbitrary $U \in C_3$. To avoid this problem, we only consider U which commutes with E to ensure that $UEU^\dagger = E \in C_2$. (We will show later there are interesting gates in C_3 even under this restriction, with appriopriate choice of X or Z teleportation circuits.) Then Eq. (10) becomes



(11)

All the circuit elements outside the dotted box can be implemented fault-tolerantly. Therefore, if we can create the logical state $UA|0\rangle^{\otimes n}$ fault-tolerantly, we can apply the gate $U \in C_3$ to any encoded state $|\psi\rangle$ fault-tolerantly.

The initial state in the dotted box consists of n encoded $|0\rangle$ states. It has stabilizers Z_i $(i = 1, \ldots, n)$, where Z_i is the encoded Pauli operator Z acting on the i^{th} encoded qubit. The stabilizers of $UA|0\rangle^{\otimes n}$ in the dotted box are $UAZ_iA^\dagger U^\dagger = UA_iZ_iA_i^\dagger U^\dagger$. Note from Eqs. (6) and (7) that $A_i = I$ and H when $D_i = Z_i$ and X_i respectively, so that $A_iZ_iA_i^\dagger = D_i$ is always true [18]. Therefore, the stabilizers of $UA|0\rangle^{\otimes n}$ are $UD_iU^\dagger$, which are in the Clifford group, and $UA|0\rangle^{\otimes n}$ can be prepared by fault-tolerant measurements of its stabilizers. This completes the discussion on how to perform the fault-tolerant gate U on any encoded state.

Using the above construction, we can systematically construct interesting gates in $C_3 - C_2$, including the $\pi/8$ gate, the controlled-phase gate and the Toffoli gate, as will be shown in Section IV.

C. Recursive construction

In this section, we discuss what gates can be constructed with one-bit teleportation as a primitive. We extend our discussion to gates in C_k and characterize a class of gates which can be recursively constructed.

We will prove by induction that the diagonal subset of C_k, defined by $F_k = \{U \in C_k \text{ and } U \text{ is diagonal}\}$, can be recursively constructed. First of all, when $U \in F_k$, we choose to apply X-teleportation to each logical qubit. In this case, each E_i is a CNOT taking the i^{th} logical qubit in the first register as control bit. Therefore E commutes with U and Eq. (11) holds. Second, for $U \in F_k$, and $D \in C_1$, $UDU^\dagger = \tilde{U}D$ where $\tilde{U} \in F_{k-1}$ [19]. If the gates in F_{k-1} can be performed, the classically-controlled operator $UDU^\dagger$ for $U \in F_k$ can also be performed. Third, it can be proved by induction that $UA|0\rangle^{\otimes n}$ can be prepared fault-tolerantly [9,20]. Finally, the gates in $F_2 \subset C_2$ have transversal implementation. By induction, all the gates in F_k can be performed fault-tolerantly by a recursive construction.

The sets F_k contain many interesting gates, such as the single qubit $\pi/2^k$ rotations, $V^k = \mathrm{diag}(1, e^{i\pi/2^k})$, and the controlled rotations, $\Lambda_1(V^{k-1}) = \mathrm{diag}(1, 1, 1, e^{i\pi/2^{k-1}})$, which are used in the quantum Fourier transform circuit [11,21] essential to Shor's factoring algorithm [11]. F_k also includes the multiple-qubit gates $\Lambda_n(V^l)$ for $n + l \leq k$ [19], where $\Lambda_n(V^l)$ applies V^l to the $(n+1)^{th}$ qubit if and only if the first n qubits are all in the state $|1\rangle$. By the closure property of F_k [19], all products of $\Lambda_n(V^l)$ for $n + l \leq k$ are in F_k. For small k, recursive construction can be more efficient than approximating these gates to an equal accuracy using a universal set of fault tolerant quantum logic gates.

The gates in F_k are not the only ones which can be constructed using the one-bit teleportation scheme. If $U \in C_3$ is related to an element in F_3 by conjugation by Hadamard gates in the i_1^{th}, ..., i_l^{th} qubits, E can be made to commute with U by applying Z teleportation to the i_1^{th}, ..., i_l^{th} qubits and X teleportation to the rest. The Toffoli gate is an example. Using the general one-bit teleportation circuits discussed in Appendix A, C_3 gates in the form $U = G_bVG_a$ for $V \in F_3$ and $G_a, G_b \in C_2$ can be performed. This strictly extends what can be achieved by X and Z teleportation only. Finally, from a physical point of view, $U = G_bVG_a$ where $V \in F_k$ and $G_a, G_b \in C_2$ can be indirectly performed, by performing V using teleportation and G_a, G_b without teleportation.

Comparing the present construction with the prior two-bit one [9], we find that with the two-bit scheme all the C_k gates can be recursively constructed, since only C_1 operators appear in the teleportation circuits. In contrast, with the present construction, the CNOT in the circuit places an additional constraint on $U \in C_k$, that $UEU^\dagger$ has to be easily performed. For example, C_3 gates

of the form $U = G_b V G_a$ for $V \in F_3$, $G_a, G_b \in C_2$ can be performed; however, it is not known if they represent all the C_3 gates. The fact X teleportation is sufficient to implement F_k gates, and all other teleportation circuits found so far only extend F_k to include extra C_2 multipliers is intriguing. However, the complicated constraint leaves us unable to strictly describe the exact capability of one-bit teleportation constructions compared to that of two-bit teleportation, and this distinction remains an interesting and difficult open question. In this paper, we concentrate on the large set of interesting gates which *can* be performed.

IV. EXAMPLES

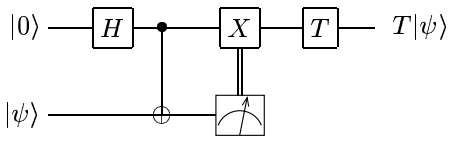
We systematically and explicitly construct three important fault tolerant gates in $C_3 - C_2$ using the general construction described in Sec. III. Any one of these gates, together with the Clifford group, form a universal set of gates.

A. The $\pi/8$ gate

The $\pi/8$ gate, T, has matrix representation

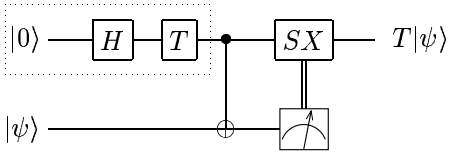
$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} . \tag{12}$$

Note that T is diagonal. Following the recipe in Sec. III, we choose to apply X teleportation to $|\psi\rangle$ and apply T to the teleported $|\psi\rangle$:



(13)

We commute T backwards using two facts. First, $TXT^\dagger = \sqrt{i}SX$, where the phase gate S (defined in Sec. III A) satisfies $S|x\rangle = i^x|x\rangle$ for $x = \{0, 1\}$. Second, T commutes with the CNOT by construction. Thus, we obtain a circuit to implement the $\pi/8$ gate (where an irrelevant overall phase has been ignored):



(14)

All the circuit elements outside the dotted box can be implemented fault-tolerantly . Furthermore, the dotted box can be replaced by the state,

$$|\phi_+\rangle = TH|0\rangle = \frac{|0\rangle + e^{i\pi/4}|1\rangle}{\sqrt{2}} , \tag{15}$$

which can be prepared fault-tolerantly as follows. Since $|0\rangle$ has stabilizer Z ($|0\rangle$ is a $+1$ eigenstate of Z), $|\phi_+\rangle = TH|0\rangle$ is a $+1$ eigenstate of W defined as

$$W = (TH)Z(TH)^\dagger = \sqrt{i}SX . \tag{16}$$

Moreover, the state $|\phi_-\rangle \equiv Z|\phi_+\rangle$ is a -1 eigenstate of W (because $\{Z, W\} = 0$, $W(Z|\phi_+\rangle) = -ZW|\phi_+\rangle = -Z|\phi_+\rangle$). To create $|\phi_+\rangle$, we first prepare the logical $|0\rangle$ state

$$|0\rangle = \frac{1}{\sqrt{2}}(|\phi_+\rangle + |\phi_-\rangle) \tag{17}$$

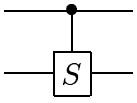
by measuring Z fault-tolerantly [1,17,5]. Second, we prepare a *cat state* $\frac{1}{\sqrt{2}}(|\bar{0}\rangle + |\bar{1}\rangle)$ [1], where $|\bar{i}\rangle$ consists of a number of physical qubits in state $|i\rangle$ $(i = 0, 1)$, and the number of physical qubits is equal to the block size of the logical state. The cat state cannot be created fault-tolerantly, but it can always be verified [1]. Third, we apply the cat-state-controlled-W to the two states prepared, $(|\bar{0}\rangle + |\bar{1}\rangle)(|\phi_+\rangle + |\phi_-\rangle)/2$. This operation applies W to $(|\phi_+\rangle + |\phi_-\rangle)$ if and only if the cat state is $|\bar{1}\rangle$. This step is guaranteed to be fault tolerant by the general construction. Specifically, since $T \in C_3$, $W \in C_2$ has a transversal implementation, hence, the cat-state-controlled-W can be implemented bitwise [9]. This leads to the following state

$$\frac{1}{2}(|\bar{0}\rangle + |\bar{1}\rangle)|\phi_+\rangle + \frac{1}{2}(|\bar{0}\rangle - |\bar{1}\rangle)|\phi_-\rangle . \tag{18}$$

Finally, a fault-tolerant measurement of $X \otimes \cdots \otimes X$ on the cat state can be made to distinguish $|\bar{0}\rangle + |\bar{1}\rangle$ and $|\bar{0}\rangle - |\bar{1}\rangle$. If the result is $|\bar{0}\rangle - |\bar{1}\rangle$, the logical state is collapsed to $|\phi_-\rangle$, which can be converted to $|\phi_+\rangle$ by applying Z. If the result is $|\bar{0}\rangle + |\bar{1}\rangle$, no operation is needed as the logical state is already in the desired state $|\phi_+\rangle$. Finally $|\phi_+\rangle$ can be verified by measuring its stabilizer W and the stabilizers of the quantum code. Thus, we have obtained the ancilla state for constructing the fault-tolerant T gate on the encoded state. We remark that we re-derive the same circuit and ancilla state used in [6].

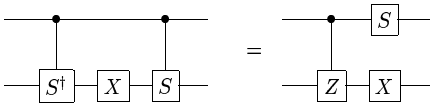
B. The controlled–phase gate

The controlled-phase gate, $\Lambda_1(S)$, (defined in Sec. III A) acts on basis states according to $\Lambda_1(S)|xy\rangle = i^{x \cdot y}|xy\rangle$ for $x, y \in \{0, 1\}$. $\Lambda_1(S) \in C_3$, and together with H and CNOT, form a universal set of gates [16,12]. We use the following circuit symbol for $\Lambda_1(S)$

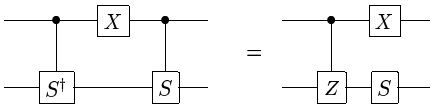


(19)

$\Lambda_1(S)$ commutes with Z_i and it transforms X_i $(i = 1, 2)$ as follows:

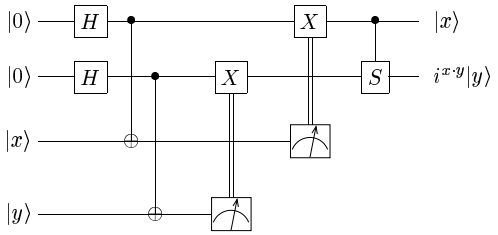


(20)



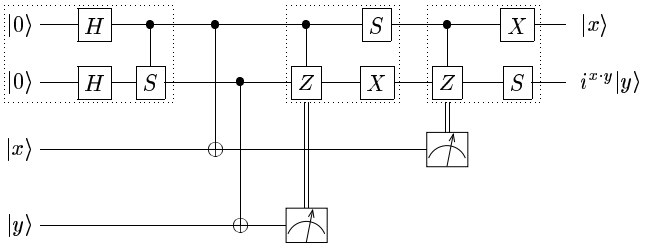
(21)

where the controlled-Z operation, $\Lambda(Z)$, acts on basis states as $\Lambda(Z)|x\rangle|y\rangle = (-1)^{x\cdot y}|x\rangle|y\rangle$. To construct $\Lambda_1(S)$, we first teleport the two-qubit state $|\psi\rangle$ and apply $\Lambda_1(S)$. This linear transformation preserves phase coherence, and thus, to understand it, it is sufficient for us to consider just its action on the basis states $|xy\rangle$. Since $\Lambda_1(S)$ is diagonal, we apply X-teleportation to both qubit states such that the CNOTs in the circuit commute with $\Lambda_1(S)$.



(22)

Commuting $\Lambda_1(S)$ backwards using the commutation rules in Eqs. (20) and (21), we obtain a circuit for the controlled-phase gate,



(23)

where the double lines control all the operations in the corresponding dotted boxes. All the circuit elements in Eq. (23), except for those in the top left dotted box, can be implemented fault-tolerantly on encoded states. It remains to prepare the state created in the top left dotted box, namely,

$$|\phi_+\rangle = \Lambda_1(S)(H_1 \otimes H_2)|00\rangle \tag{24}$$

$$= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + i|11\rangle)\,. \tag{25}$$

This can be achieved fault-tolerantly, very similarly to the ancilla preparation for the $\pi/8$ gate. Specifically, the stabilizers of $(H_1 \otimes H_2)|00\rangle$ are X_i and the corresponding stabilizers of $|\phi_+\rangle$ are $W_i = \Lambda_1(S)X_i\Lambda_1(S^\dagger)$ for $i = 1, 2$. Using the commutation rules in Eqs. (20) and (21), $W_1 = (X_1 \otimes S_2)\Lambda(Z)$ and $W_2 = (S_1 \otimes X_2)\Lambda(Z)$. They are both in C_2. Since Z_1 anticommutes with the stabilizer W_1,

$$|\phi_-\rangle \equiv Z_1|\phi_+\rangle \tag{26}$$

$$= \frac{1}{2}(|00\rangle + |01\rangle - |10\rangle - i|11\rangle) \tag{27}$$

is a -1 eigenstate of W_1. We apply a procedure similar to the ancilla preparation for the $\pi/8$ gate. First, prepare the state

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|\phi_+\rangle + |\phi_-\rangle) \tag{28}$$

$$= \frac{1}{\sqrt{2}}|0\rangle(|0\rangle + |1\rangle) \tag{29}$$

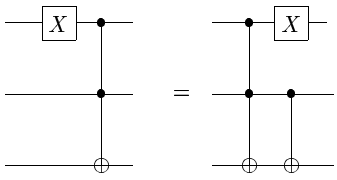
by fault-tolerantly measuring its stabilizers Z_1 and X_2. Second, prepare the cat state $\frac{1}{\sqrt{2}}(|\bar{0}\rangle + |\bar{1}\rangle)$ of physical size equal to a single block of the quantum code. Third, apply the cat-state-controlled-W_1, which applies W_1 to $|\phi\rangle$ if and only if the cat state is $|\bar{1}\rangle$. This step which measures W_1 is transversal since $W_1 \in C_2$. We obtain the state:

$$\frac{1}{2}(|\bar{0}\rangle + |\bar{1}\rangle)|\phi_+\rangle + \frac{1}{2}(|\bar{0}\rangle - |\bar{1}\rangle)|\phi_-\rangle\,. \tag{30}$$

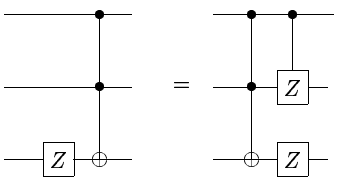
Finally, we measure $X \otimes \cdots \otimes X$ on the cat state which projects Eq. (30) onto one of the two terms. We either obtain $|\phi_+\rangle$ or $|\phi_-\rangle$, in the latter case, a further Z_1 is applied to convert the outcome to the desired ancilla state $|\phi_+\rangle$, which can then be verified by measurements of its stabilizers W_1, W_2, and other stabilizers of the code. This ancilla completes the fault-tolerant construction of the controlled-phase gate.

C. The Toffoli gate

To construct the Toffoli gate (controlled-controlled-NOT), we begin with some useful commutation rules:

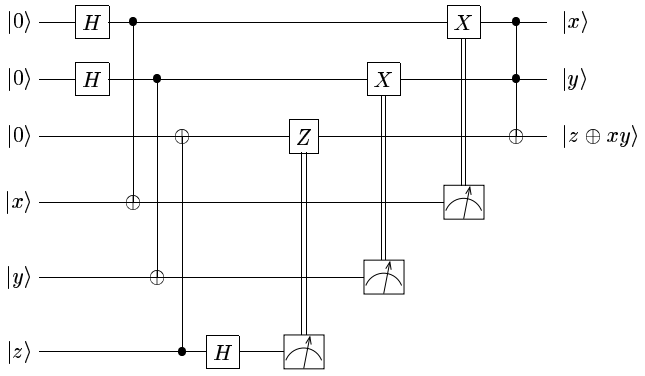


(31)



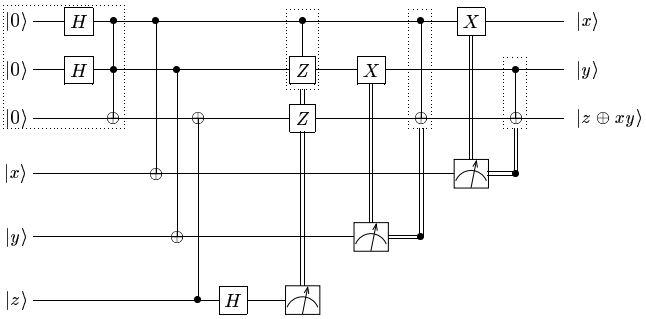
(32)

As in the controlled-phase gate construction, we demonstrate the construction on basis states $|xyz\rangle$ for three qubits. We first teleport $|xyz\rangle$ and then apply a Toffoli gate. Since the Toffoli gate is diagonalized by a Hadamard transform on the target qubit, the choice of X (Z) teleportation for the control (target) qubits ensure the three CNOTs commute with the Toffoli gate.



(33)

Commuting the Toffoli gate all the way back to the left side using Eq. (31), Eq. (32), and the commutativity with the CNOTs, we find that Eq. (33) is equivalent to



(34)

All the circuit elements except those in the left most dotted box can be implemented fault-tolerantly. It remains to prepare the state created in the dotted box,

$$|\phi_+\rangle = U(H_1 \otimes H_2)|000\rangle \tag{35}$$

$$= \frac{1}{2}(|000\rangle + |010\rangle + |100\rangle + |111\rangle)\,, \tag{36}$$

where U represents the Toffoli gate. Again, the state is prepared by fault tolerantly measuring a stabilizer of $|\phi_+\rangle$ on some standard states. Since $(H_1 \otimes H_2)|000\rangle$ has stabilizers X_1, X_2 and Z_3, $|\phi_+\rangle$ has stabilizers $W_1 = X_1 \otimes \text{CNOT}_{23}$, $W_2 = X_2 \otimes \text{CNOT}_{13}$ and $W_3 = Z_3 \otimes \text{CZ}_{12}$, where CZ represents a controlled-Z, and the *ordered* subscripts for CNOT and CZ specifies the control and target bits. The stabilizers of $|\phi_+\rangle$ are all in C_2. We next prepare a superposition of the ± 1 eigenstates of W_3. First of all, $\{W_3, X_3\} = 0$, therefore $|\phi_-\rangle = X_3|\phi_+\rangle$ is a -1 eigenstate of W_3. We prepare

$$|\phi\rangle \equiv \frac{1}{\sqrt{2}}(|\phi_+\rangle + |\phi_-\rangle) = \left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right]^{\otimes 3}\,, \tag{37}$$

with stabilizers X_i ($i = 1, 2, 3$). It can be prepared by by measuring X for each block. Second, prepare the cat state $\frac{1}{\sqrt{2}}(|\bar{0}\rangle + |\bar{1}\rangle)$ of size equal to a single block of the quantum code. Third, apply the cat-state-controlled-W_3 (fault tolerant for similar reason as other examples) to obtain

$$\frac{1}{2}(|\bar{0}\rangle + |\bar{1}\rangle)|\phi_+\rangle + \frac{1}{2}(|\bar{0}\rangle - |\bar{1}\rangle)|\phi_-\rangle\,. \tag{38}$$

Finally, measure $X \otimes \cdots \otimes X$ on the cat state to obtain either $|\phi_+\rangle$ or $|\phi_-\rangle$ and convert the latter to $|\phi_+\rangle$ by applying X_3. Verify the final state by measuring W_i and the code stabilizers. This completes the ancilla and therefore the gate construction.

Note that the ancilla and the quantum circuit derived here are the same as those in Shor's original construction [1]. The one-bit teleportation scheme elucidates the choice of ancilla state and the procedure in [1].

V. REMOTE GATE CONSTRUCTION USING ONE-BIT TELEPORTATION

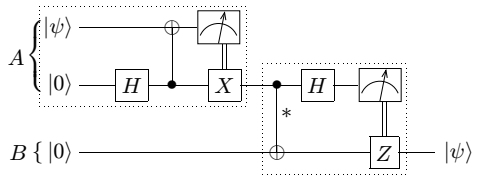
The one-bit teleportation scheme, in addition to being useful for fault-tolerant gate constructions, can also be used to design a variety of remote quantum operations. Constructing remote quantum operations is related to constructing fault-tolerant gates, in that fault-tolerance prohibits quantum operations within the same code block, while remote quantum operations prohibit quantum operations between remote parties. In the reduction from fault-tolerant gate constructions to ancilla state preparation, we first teleport the unknown state and then apply the gate. The gate is commuted backwards (in time), to effectively act on a known state. The resulting new state can be created directly. In this section, we similarly construct specific remote quantum operations, using one-bit teleportation as a basic primitive to derive both the required ancilla state and the quantum circuit. Two-bit quantum teleportation and a remote CNOT operation will be constructed.

A. Two-bit teleportation

Suppose Alice needs to send a qubit state $|\psi\rangle$ to Bob. Direct quantum communication is not allowed but Alice and Bob can share some ancilla state. The question is, how can Alice send the qubit to Bob? A well-known solution to this problem is quantum teleportation [7], which uses an EPR state and classical communication. Using one-bit teleportation, we give an alternative derivation

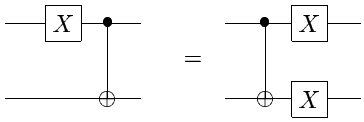
of the required (entangled) ancilla and the required teleportation circuit.

We first construct a circuit to send the unknown state with prohibited operations, then, we remove the prohibited operations. Let $|\psi\rangle$ be the state to be communicated from Alice to Bob. Alice can send $|\psi\rangle$ to Bob with two one-bit teleportations. Step 1: Alice swaps $|\psi\rangle$ with an ancilla $|0\rangle$ using X-teleportation. Step 2: Alice sends the teleported $|\psi\rangle$ to Bob using Z-teleportation (with a prohibited CNOT in this step). The circuit representation for the process is:



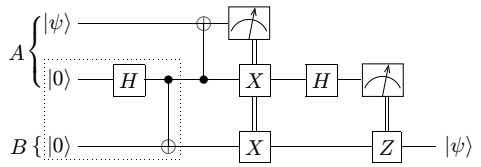
(39)

The only prohibited operation (CNOT) is marked by an asterisk. It can be commuted backwards using the commutation relation



(40)

This leads to the usual quantum teleportation circuit,



(41)

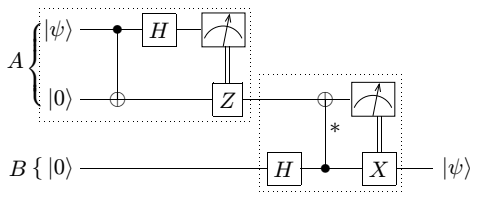
In Eq. (41) the prohibited CNOT acts only on the known state inside the dotted box. This box can be replaced by the state it creates:

$$|\phi\rangle = \Lambda_1(X)H_1|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\,, \tag{42}$$

which is the EPR state used in the original protocol. Therefore, if Alice shares this entangled state with Bob, the state $|\psi\rangle$ can be sent to Bob without quantum communication.

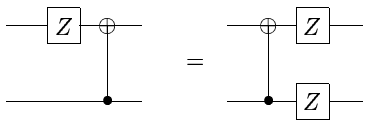
Note that the classically-controlled X on the second register only affects its overall sign, and can be omitted since the second register is subsequently measured.

An alternative circuit, which accomplishes the same task, can be derived when Z and X teleportations are used for the two steps instead. We start with the circuit:



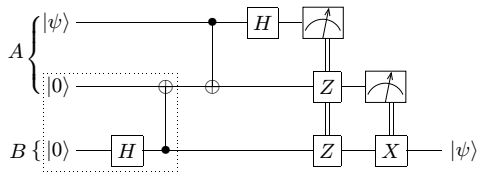
(43)

Using the commutation rule



(44)

we can commute the prohibited CNOT backwards to obtain an equivalent quantum teleportation circuit:



(45)

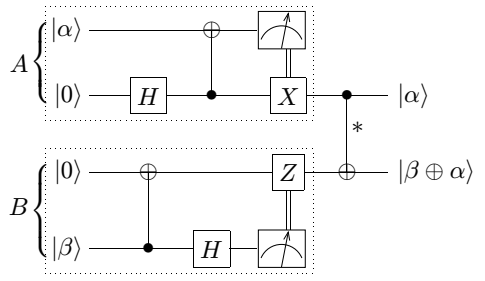
where the only disallowed element is in the dotted box, which can be replaced by the state it creates, the EPR state in Eq. (42). The irrelevant classically-controlled Z on the second register can be omitted.

Thus, we have derived the two-bit quantum teleportation circuits using one-bit teleportation as a primitive, giving further insight into how the original protocol works.

B. Remote CNOT

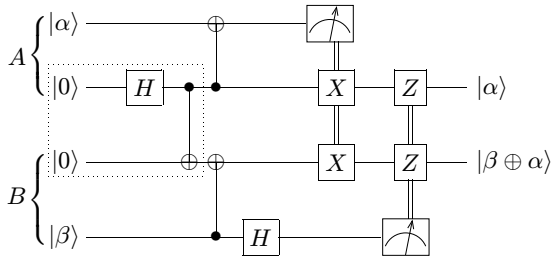
Suppose Alice and Bob have in their possession, quantum states $|\alpha\rangle$ and $|\beta\rangle$ respectively. How can they perform a simple distributed computation, a CNOT from Alice's state to Bob's state, without communicating any quantum information between them, but perhaps with the aid of some initially shared standard quantum state? A solution to this problem is given in [8]; however, the *ad-hoc* method employed does not suggest a systematic technique for deriving the solution, or solutions to generalized versions of this problem. Here, we present a general technique and derive a different circuit, which accomplishes the same task, using the one-bit teleportation scheme.

Alice and Bob can both swap their states with an ancilla state $|0\rangle$ by teleportation, and then apply a prohibited CNOT. The quantum circuit is chosen so that Alice uses X-teleportation and Bob uses Z-teleportation:



(46)

The prohibited CNOT can be commuted backwards to obtain a remote CNOT circuit:



(47)

in which the prohibited operation can be replaced by the shared EPR state in the dotted box. Provided such a shared entangled state is initially available to Alice and Bob, they can perform a remote CNOT operation.

Our construction is different from that in [8], which can also be derived using one-bit teleportation scheme, as described in Appendix B.

VI. CONCLUSION

We have presented a systematic technique to construct a variety of quantum operations, by using a primitive one-bit teleportation scheme to straightforwardly reduce quantum logic gate construction to ancilla state preparation. The usefulness of this technique is particularly manifest for two applications, fault-tolerant quantum computation, and remote quantum computation, as we have demonstrated by providing simplified constructions for the $\pi/8$, controlled-phase, and Toffoli gates, and the remote-CNOT. These constructions are easily generalized to realize an infinite family of gates. Clearly, this means that one-bit teleportation may be useful for designing and optimizing computation and communication protocols [22,23]. Even more intriguing, perhaps, is that this result gives us a first glimpse at what might someday be a standard architecture for a quantum computer: a simple assembly of one-bit teleportation primitives, capable of universal quantum computation on quantum data, given the assistance of standard quantum states which are obtained as commercial resources. Definition of such an architecture could be pivotal in the development of this field, much as the von Neumann or Harvard architectures [24] were important in classical computation.

VII. ACKNOWLEDGMENTS

The relation between fault-tolerant quantum logic gate construction and teleportation is first alluded to by Shor [1]. The X and Z teleportation circuits presented in this paper are due to Charles Bennett and Daniel Gottesman (unpublished). We are grateful to Daniel Gottesman for introducing us to the interesting subject of the C_k hierarchy, and for enlightening discussions. We thank Prof. James Harris and Prof. Yoshihisa Yamamoto for support and encouragement. This work was supported by the DARPA Ultra-scale Program under the NMRQC initiative, contract DAAG55-97-1-0341, administered by the Army Research Office. D.L. acknowledges support from the IBM Fellowship program and Nippon Telegraph and Telephone Corporation (NTT).

[1] P. Shor, Proc. 37th Ann. Symp. on Found. of Computer Science (IEEE Comp. Soc. Press) 56, (1996).
[2] J. Preskill, Proc. Roy. Soc. A: Math., Phys. and Eng. **454**, 385 (1998); LANL E-print quant-ph/9705031
[3] E. Knill, R. Laflamme, W. Zurek, Science **279**, 342 (1998).
[4] A. M. Steane, Nature **399**, 124 (1999).
[5] D. Gottesman, Phys. Rev. A **57**, (127) 1998.
[6] P. O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan, Proc. 40th IEEE Ann. Symp. on Found. of Computer Science, (1999); LANL E-print quant-ph/9906054, 1999.
[7] C. H. Bennett et al., Phys. Rev. Lett. **70**, 1895 (1993).
[8] D. Gottesman, Group 22: Proc. XXII International Colloquium on Group Theoretical Methods in Physics, eds. S. P. Corney, R. Delbourgo, and P. D. Jarvis, 32-33 (Cambridge, MA, International Press, 1999); LANL E-print quant-ph/9807006.
[9] D. Gottesman and I. L. Chuang, Nature **402**, 390 (1999); LANL E-print quant-ph/9908010.
[10] We write $UEU^\dagger$ instead of $(U\otimes I^{\otimes n})E(U^\dagger\otimes I^{\otimes n})$ for simplicity. Unimportant identity operators are suppressed throughout the paper.
[11] P. Shor, Proc. 35^{th} Ann. Symp. on Found. of Computer Science (IEEE Comp. Soc. Press) 124-134 (1994).
[12] M. A. Nielsen and I. L. Chuang, "Quantum computation and quantum information," Cambridge University Press, Cambridge, U.K. (2000).
[13] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
[14] A. Steane, Proc. Roy. Soc. Lond. A **452**, 2551 (1996).
[15] D. Gottesman, Ph. D Thesis, LANL E-print quant-ph/9705052, (1997).
[16] A. Kitaev, Russian Math. Surveys **52**, 1191 (1997).
[17] D. DiVincenzo and P. Shor, Phys. Rev. Lett. **77**, 3260 (1996)
[18] Note that the n operators $UD_iU^\dagger$ to be performed conditioned on the measurement outcomes are precisely the n stabilizers of the ancilla state $UA|0\rangle^{\otimes n}$. This coincidence is due to the structure of the teleportation circuits. See also the examples in Sec. IV.
[19] D. Gottesman, private communication.
[20] To perform operations in F_k, we need to perform operations in F_{k-1} and prepare an ancilla with stabilizers in F_{k-1}, which requires cat-state-controlled-F_{k-1} operations to be performed. We show that the last re-

quirement can be achieved recursively. Suppose the cat-state-controlled-F_{k-2} can be performed fault-tolerantly, cat-state-controlled-F_{k-1} can also be performed fault-tolerantly. This is because cat-state-controlled-F_{k-1} requires some cat-state-controlled-F_{k-2} operations to be performed, and an ancilla with stabilizers in F_{k-2}, which can be prepared using cat-state-controlled-F_{k-2}. Since cat-state-controlled-F_2 can performed fault tolerantly, all the ancilla states for gates in F_k can be recursively prepared.

[21] D. Coppersmith, IBM Research Report RC 19642 (1994).

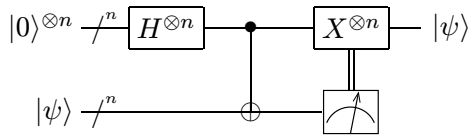
[22] R. Cleve and H. Buhrman, Phys. Rev. A **56**, 1201 (1997).

[23] R. Cleve, W. van Dam, M. Nielsen, A. Tapp, Proc. of the 1st NASA International Conference on Quantum Computing and Quantum Communications, 61 (1999); LANL E-print quant-ph/9708019.

[24] John L. Hennessey, David Goldberg, and David A. Patterson, Computer Architecture : A Quantitative Approach; Academic Press, New York (1996).

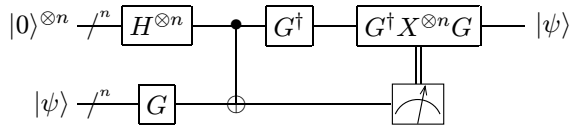
APPENDIX A: GENERALIZATIONS OF THE ONE-BIT TELEPORTATION CIRCUITS

The following circuit teleport an n-qubit state $|\psi\rangle$ with X-teleportation:



(A1)

Now, for any $G \in C_2$, the following circuit also accomplishes the same task:

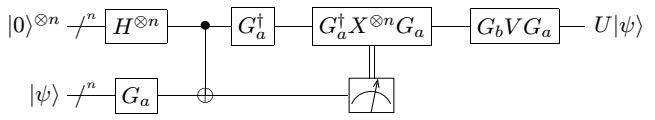


(A2)

The above circuit can be understood in the following way. It teleports $|\psi\rangle$ by first teleporting $G|\psi\rangle$ using X-teleportation, and then applying $G^\dagger$ to the teleported state. Finally, $G^\dagger$ is commuted backwards through the classically-controlled operation $X^{\otimes n}$, changing it to $G^\dagger X^{\otimes n} G \in C_1$ in Eq. (A2). When $G = I^{\otimes n}$ and $H^{\otimes n}$, Eq. (A2) reduces to X and Z teleportation circuit. Therefore, Eq. (A2) is a generalization of both one-bit teleportation circuits.

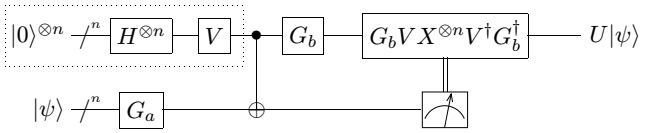
In Sec. III, we have shown that all the operations in F_3 can be performed fault-tolerantly using X-teleportation. Here, we generalize the result to show that, if $U \in C_3$ and $U = G_b V G_a$, where $V \in F_3$ and $G_a, G_b \in C_2$, then, U can be performed fault-tolerantly using the general one-bit teleportation scheme, by the following procedure:

Step 1: Using the circuit in Eq. (A2) with $G = G_a$, we first teleport the state $|\psi\rangle$ to the ancilla initialized in the state $|0\rangle^{\otimes n}$, and then apply U to the resulting state. This can be represented by:



(A3)

Step 2: Commuting U backwards, one obtains:



(A4)

Note, the new classically-controlled operation is $G_b V X^{\otimes n} V^\dagger G_b^\dagger$, which is in C_2 because $V X^{\otimes n} V^\dagger \in C_2$. Therefore, it can be performed fault-tolerantly. The remaining circuit elements can also be performed fault tolerantly, except those in the dotted box, which can be replaced by an ancilla prepared in the state $V H^{\otimes n}|0\rangle^{\otimes n}$ fault-tolerantly.

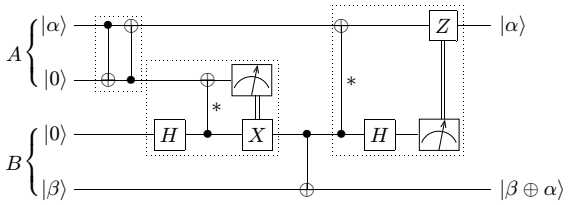
There are some C_3 gates which cannot be constructed using X and Z-teleportation directly, but can be constructed using the generalized one-bit teleportation scheme. For instance, the controlled Hadamard gate $\Lambda_1(H_2) \in C_3 - C_2$ does not commute with E for all possible combination of X and Z teleportation circuits, but $\Lambda_1(H_2)$ can be written as $G_b V G_a$ with $G_a = Q_2^\dagger$, $G_b = \Lambda_1(X_2) Q_2$ and $V = T_1 \Lambda_1(S_2^\dagger)$, where $Q = S^\dagger H S \in C_2$. Thus, $\Lambda_1(H_2)$ can still be performed using the general one-bit teleportation scheme.

Although the generalized one-bit teleportation circuit allows more operations in C_3 to be performed, they differ from an F_3 element merely by Clifford group operations, and therefore can be precisely constructed by constructing F_3 gates precisely. In fact, the efficiency of implementing $U = G_b V G_a$ using Eq. (A4) is exactly the same as applying the gates G_a, V and G_b in sequence. We have not been able to find nontrivial additional gate constructions due to the above generalized framework, but it nonetheless provides better insights on the structure of one-bit teleportation.

APPENDIX B: ALTERNATIVE REMOTE CNOT CIRCUIT

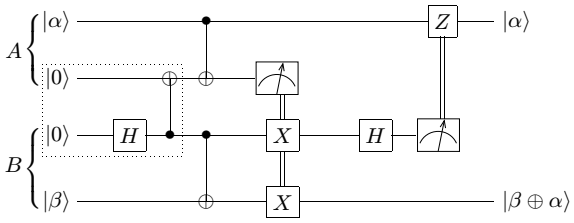
A remote CNOT between the states $|\alpha\rangle$ and $|\beta\rangle$ belonging to Alice and Bob respectively can be performed by a four step procedure: (1) Alice swaps her state $|\alpha\rangle$ with an ancilla $|0\rangle$, (2) Alice sends the teleported $|\alpha\rangle$ to Bob using X-teleportation, (3) Bob applies CNOT from

$|\alpha\rangle$ to $|\beta\rangle$, and (4) Bob teleports $|\alpha\rangle$ back to Alice using Z-teleportation. Steps (2) and (4) involve prohibited operations. Here is a circuit representation:



(B1)

The two prohibited CNOTs are labelled with asterisks. They can be commuted backwards to obtain the equivalent circuit:



(B2)

which again reduces prohibited operations to some specific shared entangled state.